Addendum au cours d'algèbre de licence à l'université de NICE en 1978-79 - Notes personnelles de Dany-Jack MERCIER

1 Relations d'ordre

Relation d'ordre, graphe d'une relation d'ordre.

Soit E un ensemble et $\leq$ une relation sur E. On dit que $(E, \leq)$ est un ensemble ordonné si :

R 1) $\forall x \in E \quad x \leq x$

A 2) $x \leq y$ et $y \leq x \Rightarrow x = y$

T 3) $x \leq y$ et $y \leq z \Rightarrow x \leq z$

[4) $x \leq y \Rightarrow x \leq x$ et $y \leq y$]

On définit le graphe d'une relation $\mathcal{R}$ par :

$$G = \{(x,y) \in E \times E \;/\; x \mathcal{R} y\}$$

Pro : Pour qu'une relation $\mathcal{R}$ définie sur E soit une relation d'ordre, il faut et il suffit que son graphe G satisfasse aux conditions :

i) $G \circ G = G$ ($\subset$ suffit)

ii) $G \cap G^{-1} = \Delta$ (diagonale)

NB : $G \circ G = \{(x,y) \in E \times E \;/\; \exists z \;\; (x,z) \in G$ et $(z,y) \in G\}$ et $\Delta = \{(x,x) / x \in E\} \subset E \times E$ est la diagonale de E.

preuve :

* Si $\mathcal{R}$ est une relation d'ordre,

$$G \circ G = \{(x,y) \;/\; \exists z \in E \;\; (x,z) \in G \text{ et } (z,y) \in G\}$$

ainsi $\forall (x,y) \in G \circ G \quad (x,y) \in G \Rightarrow G \circ G \subset G \quad (1)$

d'autre part :

$G \cap G^{-1} = \{(x,y) \;/\; (x,y) \in G$ et $(y,x) \in G\} = \Delta$

Alors $\Delta \subset G$ et donc $G = \Delta \circ G \subset G \circ G$ ce qui compte tenu de (1) donne $G \circ G = G$.

* Inversement, si l'on définit $\mathcal{R}$ par $x \mathcal{R} y \Leftrightarrow (x,y) \in G$ de façon à ce que le graphe de $\mathcal{R}$ soit G, on a :

1) $x \in E \Rightarrow (x,x) \in \Delta \subset G$
2) Si $(x,y) \in G$ et $(y,x) \in G$ alors $(x,y) \in G \cap G^{-1} = \Delta$
3) $(x,y) \in G$ et $(y,z) \in G \Rightarrow (x,z) \in G \circ G = G$

CQFD

<u>Remarque :</u> $x \leq y \Leftrightarrow (x,y) \in G$

$\mathbb{N}$

$\mathbb{N}$ muni de $\leq$: graphe de $\leq$

Élément minimal ; plus petit élément ; borne inférieure etc...

Soit $(E, \leq)$ un ensemble ordonné.

$a \in E$ est dit " élément minimal " de E si

$$\forall x \in E \quad x \leq a \Rightarrow x = a$$

$a \in E$ est dit " plus petit élément " de E (ou " minimum " de E) si :

$$\forall x \in E \quad x \geq a$$

Il est unique s'il existe.

$(E, \leq)$

X   Sup X

Borne supérieure et borne inférieure.

Soit $(E, \leq)$ un ensemble ordonné et $X \subset E$. $x \in E$ est appelé "minorant de X" si $\forall y \in X \quad x \leq y$. Par définition, la borne supérieure de X est le plus petit des majorants de X. On note Sup X.
On définit aussi les minorants de X, et Inf X.

ex: $E = \mathbb{R} \quad X =]0,1[\quad \text{Sup} X = 1$

Définitions.

Def

On dit que $(E, \leq)$ est <u>filtrant à droite</u> (resp. à gauche) si $\forall x, y \in E \quad \exists z \in E \ / \ z \geq x$ et $z \geq y$.

On dit que $(E, \leq)$ est <u>totalement ordonné</u> si $\forall x, y \in E \quad x \leq y$ ou $y \leq x$

On dit que $(E, \leq)$ est <u>bien ordonné</u> si E est ordonné et si :

$\forall X \subset E \quad X \neq \emptyset \quad$ X admet un plus petit élément.

NB : bien ordonné $\Rightarrow$ totalement ordonné.

On sait la définition des intervalles dans un ensemble E ordonné. Soient $a, b \in E \ / \ a \leq b$

$[a,b] = \{x \in E \ / \ a \leq x \leq b\}$

$[a,b[= \{x \in E \ / \ a \leq x < b\}$ etc...

On posera :

$$]\leftarrow, x] = \{y \in E / \ y \leq x\}$$
$$]\leftarrow, x[= \{y \in E / \ y < x\} \quad \text{etc...}$$

Principe de récurrence transfinie

Th | $(E, \leq)$ bien ordonné, et soit $P \subset E$ tel que :
$\forall x \in E \quad]\leftarrow, x[\subset P \Rightarrow x \in P$
Alors $P = E$

(NB : Si x_0 désigne le p.p. él. de E, on aura nécessairement $]\leftarrow, x_0[\subset P \Rightarrow x_0 \in P$.)

preuve :

Si $P \neq E$, soit $x = \text{Min}(E \setminus P)$. Alors $\forall y \quad y < x \Rightarrow y \in P$ d'où $]\leftarrow, x[\subset P \Rightarrow x \in P$ absurde.

Le théorème de Zermelo.

1°/ Préliminaire

lemme Soient E un ensemble, $\mathcal{F} \subset \mathcal{P}(E)$ et soit $p : \mathcal{F} \to E$ telle que $\forall X \in \mathcal{F} \quad p(X) \notin X$

Il existe alors une partie M de E et un bon ordre Γ sur M tels que (en désignant par $x \leq y$ la relation $(x,y) \in \Gamma$ dans M, et par S_x le segment $]\leftarrow, x[$) :

1°/ $\forall x \in M$ on a $S_x \in \mathcal{F}$ et $p(S_x) = x$

2°/ $M \notin \mathcal{F}$

preuve :

Soit $\mathcal{M} = \{ G \subset E \times E \;/$ a) G = graphe d'un bon ordre sur $pr_1 G = U$; b) si on note $x \leq y$ la relation $(x,y) \in G$ dans U, $\forall x \in U \quad S_x \in \mathcal{F}$ et $p(S_x) = x$ $\}$

A | Montrons que, si $G \in \mathcal{M}$ et $G' \in \mathcal{M}$ et si $\begin{cases} pr_1 G = U \\ pr_1 G' = U' \end{cases}$ on a $U \subset U'$ ou $U' \subset U$
Et que si, par exemple, $U \subset U'$, alors $G = G' \cap (U \times U)$ (c.à.d la relation d'ordre sur U est induite par la relation d'ordre sur U') et U est un segment de U' (du type $]\leftarrow, x[$)

Pour cela, considérons $V = \{ x \in U \cap U' \;/$ $S_x = S'_x$ et les ordres induits sur ce segment par ceux de U et U' soient identiques $\}$

• V est un segment dans U et dans U' [en effet, si $x \in V$ $y \underset{U}{\leq} x \Rightarrow y \in V$ puisque, U étant bien ordonné, si $U \setminus V = \emptyset$ $V = U$ est un segment, sinon $U \setminus V \neq \emptyset \Rightarrow \exists\, \alpha = \mathrm{Min}(U \setminus V)$ et alors $]\leftarrow, \alpha[= V$ dans U]
et les ordres induits sur V sont les mêmes, [si $x, y \in V$, alors $S_x = S'_x$ et $S_y = S'_y$ et les ordres induits sur ces segments sont les mêmes. U bien ordonné $\Rightarrow$ par ex $x \underset{U}{\leq} y \Rightarrow x \in \underset{U}{]}\leftarrow, y]$ et $\underset{U}{]}\leftarrow, y] = \underset{U'}{]}\leftarrow, y] \Rightarrow x \underset{U'}{\leq} y$]

• Montrons que $V = U$ ou $V = U'$ [notre assertion A| sera alors prouvée puisque si $V = U$, $\forall x \in U$ $x \in V \subset U'$ donc $U \subset U'$; et $x \underset{U}{\leq} y$ $x, y \in U \Rightarrow x, y \in V \Rightarrow$ l'ordre est le même que l'ordre de U'. Donc $x \underset{U'}{\leq} y$. En d'autres termes $G = G' \cap (U \times U)$]

Raisonnons par l'absurde en supposant que $V \neq U$ et $V \neq U'$.

Soit $\begin{cases} x = \underset{U}{\mathrm{Min}}\, U \setminus V & (U \text{ bien ordonné}) \\ x' = \underset{U'}{\mathrm{Min}}\, U' \setminus V & (U' \quad " \quad) \end{cases}$

On a $V = S_x$ dans U et $V = S_{x'}$ dans U', et par hypothèse : $V \in \mathcal{F}$ et $\begin{cases} x = p(S_x) \\ x' = p(S_{x'}) \end{cases}$

d'où $x = x' \Rightarrow x \in V$ ce qui est absurde.

Considérons $M = \bigcup_{G \in \mathfrak{M}} pr_1 G$

Compte tenu de l'assertion A), il existe un ordre et un seul sur M qui induise sur chacun des $pr_1 G$ l'ordre donné. Muni de cet ordre, M est bien ordonné.
Alors :

1°/ On a
$\forall x \in M \quad S_x \in \mathcal{F}$ et $p(S_x) = x$

2°/ Si $M \in \mathcal{F}$, soit $p(M) = a \notin M$.
Considérons $M' = M \cup \{a\}$ et disons que a est le plus grand élément de M'. M est alors bien ordonné. Comme $M = S_a$ (dans M'), on aurait :

$$S_a \in \mathcal{F} \quad \text{et} \quad p(S_a) = a \notin S_a$$

Ainsi, le graphe de $M' \in \mathfrak{M}$, ce qui est absurde car $M' \supsetneq M$.

CQFD

2°/ Théorème de Zermelo.

Th | Sur tout ensemble E, il existe un bon ordre.

preuve : Soit $\mathcal{F} = \mathcal{P}(E) \setminus \{E\}$ et $p : \mathcal{F} \longrightarrow E$
$x \longmapsto z_x$

où $z_x \in E \setminus X$.
On a : $\forall X \in \mathcal{F} \quad p(X) \notin X$.
On peut appliquer le lemme précédent :
$\exists M \subset E \quad \exists$ bon ordre sur M tel que
$p(S_x) = x \quad \forall S_x \in \mathcal{P}(E)$
et tel que $M \notin \mathcal{F} \Rightarrow M = E$.
CQFD

Ensembles inductifs

1°/ Définition

Def | On dit qu'un ensemble ordonné $(E, \leq)$ est inductif si toute partie totalement ordonnée de E possède un majorant dans E.

2°/ Théorème de Zorn

Th | Tout ensemble ordonné inductif possède un élément maximal

démonstration :
v est appelé majorant strict de $X \subset E$ si v est un majorant de X et si $v \notin X$.

Posons $\mathcal{F}' = \{ S \in \mathcal{P}(E) \ / \ S$ possède 1 maj. strict $\}$

$$p : \mathcal{F}' \longrightarrow E$$
$$S \longmapsto \tau_S \ (= \text{“un” majorant strict de } S)$$

Alors $p(S) = \tau_S \notin S$ et on peut appliquer le lemme du § précédent :

$\exists M \subset E \quad \exists$ bon ordre Γ sur M satisfaisant à :

$$\begin{cases} \forall x \in M \quad S_x \in \mathcal{F}' \text{ et } p(S_x) = x \\ \text{et} \quad M \notin \mathcal{F}' \end{cases}$$

<u>L'ordre Γ est identique à l'ordre induit sur M par E</u> :

En effet, $\{(x,y) \in \Gamma \text{ et } x \neq y\} \Leftrightarrow x \in S_y$

Comme $p(S_y) = y$ est un majorant strict de S_y (pour l'ordre de E), on a : $x < y$ dans E.

Ainsi $\{(x,y) \in \Gamma \text{ et } x \neq y\} \Rightarrow x \underset{E}{<} y$

Inversement, soit $x, y \in M \ / \ x \underset{E}{<} y$. ~~Si~~ M est totalement ordonné par Γ, donc $(x,y) \in \Gamma$ ou $(y,x) \in \Gamma$. Si $(y,x) \in \Gamma$ alors $y \underset{E}{\leq} x$ ce qui est absurde. Donc $(x,y) \in \Gamma$ et $x \neq y$.

On a montré que

$$\{(x,y) \in \Gamma \text{ et } x \neq y\} \Leftrightarrow x \underset{E}{<} y$$

oui : les 2 ordres coïncident.

Cela étant, $\exists m$ majorant de M dans E, par hypothèse. (E inductif).

Comme $M \notin \mathcal{F}'$, M n'admet pas de majorants stricts, donc $m \in M$ et m est un élément maximal dans E

CQFD

Co 1 | Soient E un ensemble ordonné inductif, et $a \in E$. Il existe un élément maximal m de $E \ / \ m \geq a$

On prend $F = \{x \in E / x \geqslant a\}$. F est ordonné inductif, et possède donc un élément maximal qui est aussi un élément maximal de E.

Co 2 | Soit $(\mathcal{P}(E), \subset)$ et $\mathcal{F} \subset \mathcal{P}(E)$ tel que, pour tout sous-ensemble $\mathcal{S}$ de $\mathcal{F}$, totalement ordonné par l'inclusion, $\bigcup_{s \in \mathcal{S}} s \in \mathcal{F}$ (resp. $\bigcap_{s \in \mathcal{S}} s \in \mathcal{F}$).

Alors $\mathcal{F}$ possède un élément maximal (resp. minimal)

Décomposition d'un groupe commutatif fini

I Définition d'un p-groupe

Def | Soit G un groupe. On dit que G est un p-groupe si son cardinal est une puissance de p ($p \in \mathcal{P}$).

Th | Soit G un groupe commutatif fini.
Alors $G = p\text{-groupe} \iff \{ \forall x \in G \ \exists \alpha \in \mathbb{N} \ / \ \omega(x) = p^\alpha \}$

preuve : • Supposons que $\forall x \in G \ \omega(x) = p^\alpha$. On fait une récurrence sur le cardinal de G. En notation additive :
→ Pour $G = \{0\}$, c'est évident
→ Soit G de cardinal n. Soit $x \in G$, $x \neq 0$. Notons $H = \langle x \rangle$. C'est un groupe cyclique d'ordre p^k. Mais $\# G = \# H \cdot \# G/_H$ et $G/_H$, groupe commutatif, vérifie $\forall \dot{x} \in G/_H \ \exists \alpha \ / \ p^\alpha \dot{x} = \dot{0}$. De plus $\# G/_H < \# G$. L'hypothèse de récurrence s'applique : $\# G/_H = p^\beta$. Comme $\# H = p^k$, on trouve que $\# G = p^{\beta + k}$ cqFd
• Inversement, si G est un p-groupe, $\# G = p^k$ et tout élément x de G engendre $\langle x \rangle$ d'ordre $p^\alpha \mid p^k$. Par suite $\omega(x) = p^\alpha$.

II Décomposition en p-groupes (ou "composantes p-primaires")

Th | Soit G un groupe commutatif fini d'ordre $n = p_1^{r_1} \cdots p_k^{r_k} = q_1 \cdots q_k$
Posons $G(p_i) = \{ x \in G \ / \ q_i x = 0 \}$
$G(p_i)$ est un p_i-groupe et :

$$G = G(p_1) \oplus \cdots \oplus G(p_k)$$

Il est clair que $G(p_i)$ est un groupe, et que $\forall x \in G(p_i) \quad \omega(x) \mid p_i^{r_i} \Rightarrow \omega(x) = p_i^\alpha$
donc $G(p_i) = p_i$-groupe.
Montrons la somme directe :
* $\forall x \in G \quad \exists x_i \in G(p_i) \ / \ x = x_1 + \cdots + x_k$?
Il est clair que $\Delta\left(\frac{n}{q_1}, \frac{n}{q_2}, \ldots, \frac{n}{q_k}\right) = 1 \iff \sum_{i=1}^{k} m_i \frac{n}{q_i} = 1$ (Bezout)

$$\text{Donc } x = \underbrace{m_1 \frac{n}{q_1} x}_{\in G(p_1)} + \cdots + \underbrace{m_k \frac{n}{q_k} x}_{\in G(p_k)}$$

Donc $G = G(p_1) + \cdots + G(p_k)$
* $\forall j \in [1, k] \quad G(p_1) + \cdots + G(p_{j-1}) \cap G(p_j) = \{0\}$?
Soit $x \in G(p_1) + \cdots + G(p_{j-1}) \cap G(p_j)$ où $j \in [1, k]$
Alors $q_j x = 0$ et $x = x_1 + \cdots + x_{j-1}$ où $x_i \in G(p_i) \iff q_i x_i = 0 \quad \forall i$
Soit $s = \prod_{i=1}^{j-1} q_i$. On a $sx = 0$

q_j et s sont premiers entre eux ! donc $\lambda q_j + \mu s = 1 \Rightarrow x = \lambda q_j x + \mu s x = 0$

CQFD

III Décomposition en p-groupes cycliques.

Énonçons tout d'abord :

Th 1 | Tout p-groupe commutatif G se décompose en groupes cycliques p-primaires,

$$G \simeq \mathbb{Z}/_{p^{\alpha_1}\mathbb{Z}} \times \dots \times \mathbb{Z}/_{p^{\alpha_s}\mathbb{Z}} \qquad \alpha_1 \leq \dots \leq \alpha_s$$

De plus, la suite $(\alpha_1, \dots, \alpha_s)$ est unique.

Soit G un p-groupe commutatif. Énonçons 2 lemmes :

<u>lemme 1</u> : $\left.\begin{array}{l} b \in G \quad b \neq 0 \quad p^k b \neq 0 \\ \omega(p^k b) = p^m \end{array}\right\} \Rightarrow \omega(b) = p^{m+k}$

<u>lemme 2</u> : $a_1 \in G \quad G_1 = \langle a_1 \rangle \quad \# G_1 = p^{r_1} = \operatorname{Sup}\{\omega(x) / x \in G\}$

Soit $\dot{b} \in G/_{G_1}$ tel que $\omega(\dot{b}) = p^r$. On pose $\pi_1 : G \to G/G_1$

Alors $\exists b \,/\, \pi_1(b) = \bar{b}$ et $\omega(b) = p^r$.

<u>preuve lemme 1</u> : On a $\left\{\begin{array}{l} p^{m+k} b = 0 \\ p^{m+k-1} b = p^{m-1}(p^k b) \neq 0 \text{ car } \omega(p^k b) = p^m \quad (m \geq 1) \end{array}\right.$

donc $\omega(b) = p^{m+k}$

<u>preuve lemme 2</u> : Soit $b \in G$ tel que $\pi_1(b) = \bar{b}$. π_1 est un morphisme de groupes, donc il abaisse les ordres des éléments : $\omega(b) \geq p^r$, $\forall b \in \pi_1^{-1}(\bar{b})$. $(*)$

On a $p^r b \in G_1 \iff p^r b = n\, a_1$ où $0 \leq n < p^{r_1}$

$p^r b = p^k \mu a_1$ où $p \nmid \mu \quad (k < r_1)$

$\omega(p^k \mu a_1) = \dfrac{p^{r_1}}{\Delta(p^k\mu, p^{r_1})} = p^{r_1 - k}$ et $p^r b \neq 0 \Rightarrow \omega(b) = p^{r + r_1 - k}$ (lemme 1)

Comme $r_1 = \operatorname{Sup}\{\omega(x) / x \in G\}$ et que $\omega(b) = p^{r+r_1-k}$, on aura forcément l'inégalité : $r + r_1 - k \leq r_1 \iff r \leq k$

Par suite : $p^r b = p^k \mu a_1 \Rightarrow (b - p^{k-r}\mu a_1) p^r = 0 \Rightarrow \omega(b - p^{k-r}\mu a_1) = p^r$ (cf. $(*)$)

On a qu'à prendre $b' = b - p^{k-r}\mu a_1 \in \pi^{-1}(\dot{b})$

<u>preuve du théorème</u> :

- <u>Existence de la décomposition</u>

$\# G = p^u$. On fait une récurrence sur u.

C'est vrai pour $u = 1$. Soit G de cardinal $\# G = p^u$. Alors $\# G/_{G_1} = p^{u - r_1}$ et l'on peut appliquer l'hypothèse de récurrence :

$$G/_{G_1} = \bar{G}_2 \oplus \dots \oplus \bar{G}_s \quad \text{où } \bar{G}_i = \dot{a}_i \mathbb{Z} \quad \omega(\dot{a}_i) = p^{r_i}$$

(groupes cycliques primaires)

D'après le lemme 2 :

$$\exists a_i \in G \;/\; \pi(a_i) = \dot{a}_i \text{ et } \omega(a_i) = p^{r_i}$$

Posons $G_i = a_i \mathbb{Z} = \langle a_i \rangle$ et montrons que $G = G_1 \oplus \dots \oplus G_s$:

1) $G = G_1 + \dots + G_s$

En effet, $\forall x \in G \quad \dot{x} = m_2 \dot{a}_2 + \dots + m_s \dot{a}_s \iff x = \overbrace{m_1 a_1}^{\in G_1} + \dots + m_s a_s$.

2) Si $m_1 a_1 + \dots + m_s a_s = 0 \qquad 0 \leq m_i < p^{r_i}$

alors $m_2 \dot{a}_2 + \dots + m_s \dot{a}_s = 0$ d'où $m_2 = \dots = m_s = 0$ et $m_1 a_1 = 0 \Rightarrow m_1 = 0$

Donc $G = G_1 \oplus \dots \oplus G_s \qquad G_i$ = groupe cycliques primaires d'ordre p^{α_i}

- <u>Unicité de la suite $(\alpha_1, \dots, \alpha_s)$</u>

On a $G \simeq (\mathbb{Z}/_{p\mathbb{Z}})^{m_1} \times \dots \times (\mathbb{Z}/_{p^t\mathbb{Z}})^{m_r}$

Montrons que cette décomposition est unique.

On note $G[p] = \{x \in G \,/\, px = 0\}$ = "p-groupe élémentaire de G" = groupe d'ordre p.
Cela étant défini, on a :

$$p^k G \simeq p^k \left(\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_{k+1}} \times \dots \times p^k \left(\mathbb{Z}/p^t\mathbb{Z}\right)^{m_t}$$
$$\simeq \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_{k+1}} \times \dots \times \left(p^k\mathbb{Z}/p^t\mathbb{Z}\right)^{m_t}$$

Donc $$p^k G \cap G[p] \simeq \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_{k+1}} \times \left(p^{k+1}\mathbb{Z}/p^{k+2}\mathbb{Z}\right)^{m_{k+2}} \times \dots \times \left(p^{t-1}\mathbb{Z}/p^t\mathbb{Z}\right)^{m_t} \quad (1)$$

On sait que $\left(p^k\mathbb{Z}/p^{i+1}\mathbb{Z}\right) / \left(p^i\mathbb{Z}/p^{i+1}\mathbb{Z}\right) \simeq p^k\mathbb{Z}/p^i\mathbb{Z}$ et que, dans un groupe ~~multipli~~ commutatif :

$$(H \times H') / (K \times K') \simeq H/K \times H'/K'$$

(cf 2.12 Bouvier).
La ligne (1) donne :

$$\Lambda_k = p^k G \cap G[p] / p^{k+1} G \cap G[p] \simeq \left(p^k\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^{m_{k+1}}$$
$$\simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^{m_{k+1}}$$

Ce qui prouve que Λ_k est un p-groupe élémentaire. C'est donc un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$. Λ_k qui ne dépend que du groupe G et de k, a pour dimension m_{k+1} sur $\mathbb{Z}/p\mathbb{Z}$. Donc m_{k+1} est indépendant de la décomposition choisie.
Ainsi, si nous avons : $G \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times \dots \times (\mathbb{Z}/p^t\mathbb{Z})^{m_t} \simeq (\mathbb{Z}/p\mathbb{Z})^{m'_1} \times \dots \times (\mathbb{Z}/p^{t'}\mathbb{Z})^{m'_{t'}}$

où $t \leq t'$, on aura nécessairement
$$m_k = m'_k = \dim \Lambda_k \qquad \forall k \in \mathbb{N} \text{ (en particulier } k \in [1, t'] \text{)}.$$
D'où l'unicité de la décomposition.

CQFD

Th | Soit G un groupe commutatif fini de cardinal $n = p_1^{n_1} \dots p_k^{n_k}$.
G est décomposable en groupes cycliques primaires :

$$G \simeq \mathbb{Z}/p_1^{\alpha_{11}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_1^{\alpha_{1n_1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_{k1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_{kn_k}}\mathbb{Z}$$

où $\begin{cases} p_1 < p_2 < \dots < p_k \\ \alpha_{i1} \leq \dots \leq \alpha_{in_i} \end{cases}$

De plus, cette décomposition est unique, en ce sens que la suite $(p_1^{\alpha_{11}}, \dots, p_1^{\alpha_{1n_1}}, \dots, p_k^{\alpha_{k1}}, \dots, p_k^{\alpha_{kn_k}})$ est parfaitement déterminée.

Def | $(p_1^{\alpha_{11}}, \dots, p_k^{\alpha_{kn_k}})$ s'appelle le "type de G".

preuve :
Ce théorème nous révèle la structure de tout groupe commutatif fini. Il se démontre en utilisant le 1er théorème de décomposition de G en groupes primaires (pas nécessairement cycliques), et le Th 1 précédent.

<u>existence</u> : D'après le § II,
$$G = G(p_1) \oplus \dots \oplus G(p_k)$$
D'après le Th 1 :
$$G(p_i) \simeq \mathbb{Z}/p_i^{\alpha_{i1}} \times \dots \times \mathbb{Z}/p_i^{\alpha_{in_i}}$$

unicité :

Application :

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est de type $(2,2)$

$\mathbb{Z}/4\mathbb{Z}$ est de type (2^2)

$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$ est de type $(2^3, 2^4, 3^2, 5^3)$

Remarquons bien que, si G est d'ordre $2^7 \times 3^2 \times 5^3 = 14\,400$ dans l'exemple précédent, son type est $(2^3, 2^4, 3^2, 5^3)$ et n'a donc rien à voir avec le k-uplet $(p_1^{r_1}, \dots, p_k^{r_k})$ de la décomposition de n en facteurs premiers.
Toutefois, puisque $n = \# G = \prod_{i,j} \# (\mathbb{Z}/p_i^{\alpha_{ij}}\mathbb{Z})$, on trouve que :

$$r_h = \sum_{j=1}^{n_h} \alpha_{hj} \quad \forall h \in [1, k].$$

Pro | Deux groupes abéliens finis sont isomorphes ssi ils sont de même type

preuve : Si G et G' sont de m̂ type, ils sont isomorphes. Inversement, si $G \simeq G'$, notons $\varphi : G \xrightarrow{\sim} G'$.
Soit $G \simeq \bigotimes_{i=1}^{m} \Gamma_i$ et $G' \simeq \bigotimes_{i=1}^{m'} \Gamma'_i$ les décompositions de G et G' en groupes cycliques primaires.

$\bigotimes_{i=1}^{m} \varphi(\Gamma_i)$ est une décomposition de G' en groupes cycliques primaires.
D'après le théorème précédent, (càd d'après l'unicité des types) $m = m'$ et les types de G et G' sont les mêmes.

IV Décomposition en groupes cycliques.

Th | Tout groupe commutatif fini G est isomorphe à un produit direct de groupes cycliques non nuls tels que :

$$\begin{cases} G \simeq H_1 \times H_2 \times \dots \times H_r \\ \# H_r \mid \# H_{r-1} \mid \dots \mid \# H_1 \end{cases}$$

La décomposition est unique, en ce sens que si $G \simeq K_1 \times \dots \times K_s$ et $\# K_s \mid \dots \mid \# K_1$, alors $r = s$ et $K_i \simeq H_i \ \forall i$

démonstration : D'après le th. précédent

$$G \simeq \mathbb{Z}/p_1^{\alpha_{11}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_1^{\alpha_{1n_1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_{k1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_{kn_k}}\mathbb{Z}$$

Pour tout p_i intervenant dans cette décomposition, posons

$$\beta_i = \sup_j \alpha_{ij}$$

et soit $H_1 = \prod_i \mathbb{Z}/p_i^{\beta_i}\mathbb{Z} \simeq \mathbb{Z}/\prod_i p_i^{\beta_i}\mathbb{Z}$ (théorème Chinois)

H_1 est cyclique et $G \simeq H_1 \times G_1$ où G_1 est un produit de groupes cycliques primaires $\mathbb{Z}/p_i^{\alpha_{ij}}\mathbb{Z}$ tels que, $\forall i$, $\alpha_{ij} \leq \beta_i$.

On pose alors $\gamma_i = \sup \alpha_{ij}$ (pris parmi les α_{ij} restants).

On pose :

$$H_2 = \prod_i \mathbb{Z}/p_i^{\gamma_i}\mathbb{Z} \simeq \mathbb{Z}/\prod_i p_i^{\beta_i}\mathbb{Z}$$ est cyclique, et

$$G \simeq H_1 \times H_2 \times G_2 \quad \text{où} \quad \# H_2 \mid \# H_1 .$$

Comme G est fini, le procédé l'est aussi.

<u>Unicité</u> : Si $G \simeq K_1 \times \dots \times K_s$ où les K_i vérifient les conditions de l'énoncé, chaque K_i est isomorphe à un produit de groupes cycliques primaires $\mathbb{Z}/p_i^{\beta_{ij}}\mathbb{Z}$. On obtient donc 2 décompositions en produit de groupes cycliques primaires.

Donc : (§ III) $\alpha_{ij} = \beta_{ij}$ $\forall i, j$

D'autre part, comme $|K_{i+1}|$ divise $|K_i|$, $\# K_1$ est le produit des $p_i^{\beta_{ij}}$ avec β_{ij} maximum, donc $\# K_1 = \# H_1$.
De même $\# K_2 = \# H_2$, etc...

CQFD

<u>Remarque Fondamentale</u> :

On a vu 3 théorèmes de décomposition d'un groupe commutatif fini ; il ne faut pas les confondre !

- (II) en somme directe de groupes primaires (non nécessairement cycliques)
- (III) en groupes cycliques primaires
- (IV) en groupes cycliques (non nécessairement primaires)

$$G = G(p_1) \oplus \dots \oplus G(p_k) \qquad \text{(cf paragraphe II)}$$

et en utilisant le Th 1 ci-dessus :

$$G(p_i) \simeq \mathbb{Z}/p_i^{\alpha_{i1}} \times \dots \times \mathbb{Z}/p_i^{\alpha_{in_i}}$$

L'unicité de la décomposition $(p_1^{\alpha_{11}}, \dots, p_k^{\alpha_{kn_k}})$, qui détermine le type de G, est dû :

1) à l'unicité de la suite du th. 1 : $(p_i^{\alpha_{i1}}, \dots, p_k^{\alpha_{kn_k}})$ est unique.

2) à la remarque suivante : $G = G(p_1) \oplus \dots \oplus G(p_k)$

Si G_i est p_i-primaire cyclique, alors $\forall x \in G_i \quad p_i^{\# G_i} x = 0$, donc $x \in G(p_i) = \{x \in G \,/\, p_i^{n_i} x = 0\}$. Ainsi $G_i \subset G(p_i)$

CQFD

Groupes opérant sur un ensemble.

Définition - Equation des classes.

On dit qu'un groupe G opère sur un ensemble E, à gauche, si ∃ loi externe

$$\begin{array}{rcl} G \times E & \longrightarrow & E \\ (g, x) & \longmapsto & g.x \end{array}$$

qui vérifie : 1) $g.(g'.x) = (gg').x$ $\quad \forall g, g' \in G \ \forall x \in E$

2) $e.x = x$ $\quad \forall x \in E$

Th | L'ensemble E est un G-ensemble si et seulement si G est homomorphe au groupe S(E)

NB : S(E) est le groupe symétrique de E, c.à.d le groupe de toutes les permutations de E dans E, muni de o.
L'homomorphisme $T : G \to S(E)$ annoncé n'est autre que $T_g(x) = g.x$.

Définitions :

a) G opère fidèlement sur E si $T : G \to S(E)$ est injectif,
c.à.d si $gx = x \ \forall x \in E \Rightarrow g = e$

b) $G_x = \{ y \in E / \exists g \in G \ \ y = g.x \}$ = orbite de x pour le groupe G.

c) $H_x = \{ g \in G / gx = x \}$ est un sous-groupe de G. C'est le sous-groupe d'isotropie, ou "stabilisateur" de x dans G.

Th | Soit Ω une orbite pour G. Si x et y sont éléments de Ω, alors les groupes d'isotropie H_x et H_y sont conjugués dans G.

On remarque que la relation dans E : $x \sim y \Leftrightarrow \exists g \in G \ \ y = gx$ est une relation d'équivalence, et que les classes de ~ ne sont autres que les orbites dans E :
plus précisemment : $\dot{x}_{(\sim)} = G_x$
Les orbites de E forment donc une partition de E.
Montrons le théorème :

$$x, y \in \Omega = G_z \Leftrightarrow \exists \sigma \in G \quad x = \sigma.y$$

Donc :

$$h \in H_x \Leftrightarrow h.x = x \Leftrightarrow (h\sigma).y = \sigma.y \Leftrightarrow (\sigma^{-1}h\sigma).y = y$$
$$\Leftrightarrow \sigma^{-1}h\sigma \in H_y \Leftrightarrow h \in \sigma H_y \sigma^{-1}$$

d'où $H_x = \sigma H_y \sigma^{-1}$, ce qui signifie que le sous-groupe H_x est le conjugué de H_y.
CQFD

Considérons $f_x : G \longrightarrow E$ (x fixé)
$g \longmapsto g.x$

f_x se factorise canoniquement puisque :

$$f_x(g_1) = f_x(g_2) \Leftrightarrow g_1.x = g_2 x \Leftrightarrow g_2^{-1}g_1.x = x \Leftrightarrow g_2^{-1}g_1 \in H_x$$

Ainsi, le diagramme suivant est commutatif :

$$\begin{array}{ccc} G & \xrightarrow{f_x} & f_x(G) = G_x \\ \pi \downarrow & \nearrow & \\ G/H_x & & \theta \text{ bijectif.} \end{array}$$

G/H_x : classes à gauche suivant le sous-groupe d'isotopie H_x.

Ainsi, si G est finie : $\# G_x = \# G/H_x = \dfrac{\# G}{\# H_x}$

$$\boxed{\# G_x = \frac{\# G}{\# H_x}}$$

Equation des classes :

Si l'ensemble E est fini, chaque orbite est un ensemble fini. Si $E' \subset E$, E' ne contient qu'un élément et un seul de chaque orbite, alors, eu égard à la partition réalisée par la relation $\sim$ dans E :

$$\boxed{\# E = \sum_{x \in E'} \# G_x = \sum_{x \in E'} \frac{\# G}{\# H_x}}$$ (équation des classes)

Exemple : G groupe fini. $\varphi : G \longrightarrow Int(G) \subset S(G)$
$g \longmapsto \varphi_g \ / \ \varphi_g(x) = gxg^{-1}$

φ est un épimorphisme de groupes.
C'est donc un G-ensemble pour la loi dite de conjugaison : $G \times G \longrightarrow G$
$(g, x) \mapsto gxg^{-1}$

H_x = stabilisateur de x = $\{ g \in G \ / \ gx = xg \}$

Si $z \in Z(G)$ $H_z = G$ et réciproquement. Donc $\# G_z = 1$

L'équation des classes implique : $\# G = \sum_{x \in Z(G)} \# G_x + \sum_{x \in A} \# G_x$

(A = ensemble des éléments de G tel que 2 éléments quelconques de A ne sont pas conjugués). Ainsi :

$$\boxed{\# G = \# Z(G) + \sum_{x \in A} \# G_x}$$

exercice : $p \in \mathcal{P}$, G groupe d'ordre p^k. Alors $Z(G)$ n'est pas trivial.
[Sol : Pour $x \notin Z(G)$, Card G_x divise proprement p^k donc est une puissance de p.
On a $\# Z(G) = \# G - \sum_{x \notin Z(G)} \# G_x \Rightarrow \# Z(G) \equiv 0 \ [p] \Rightarrow Z(G)$ non trivial]
(Théorème de Burnside)

Groupes primaires, groupes de Sylow

1°/ Définitions et premières propriétés.

Th 1 | Tout groupe fini commutatif contient un élément d'ordre $p \in \mathcal{P}$ si $p | \# G$
(cf ALG 10/2/80)

Th 2 | Soit G un groupe fini d'ordre n, et $p \in \mathcal{P}$ / $p^k | n$.
Alors G contient un sous-groupe d'ordre p^k

preuve : le théorème est trivial si $n = p^k$.
On raisonne par récurrence sur n en supposant le théorème vrai pour tous les groupes d'ordre $n' < n$.
G est un G-ensemble pour la loi de conjugaison $(g, x) \longmapsto g x g^{-1}$.
De 2 choses l'une :

a) $\exists x \notin Z(G) / \# G_x \not\equiv 0 \, [p]$. Alors $n = \# H_x \cdot \# G_x$
p, premier, est premier avec tout nombre qu'il ne divise pas. Donc $\Delta(p^k, \# G_x) = 1$ et le théorème de Gauss donne : $p^k | \# H_x$. H_x, stabilisateur de x, est un sous-groupe de G d'ordre $\# H_x = \frac{n}{\# G_x} < n$ puisque $\# G_x > 1$.
D'après l'hyp. de récurrence :

H_x possède un sous-groupe d'ordre p^k

b) $\forall x \notin Z(G) / \# G_x \equiv 0 \, [p]$.
L'équation des classes donne :

$$\# Z(G) = n - \sum_{x \in A} \# G_x \equiv 0 \quad [p]$$

Le centre Z(G) n'est pas trivial. Comme $p | \# Z(G)$, il existe selon le th. 1 un élément $a \in Z(G)$ d'ordre p. Le groupe $\langle a \rangle = H$ est d'ordre p. Il est distingué dans G, puisque $H \subset Z(G)$.

$p^k | n \Rightarrow p^{k-1} | \# (G/_H)$

D'après l'hypothèse de récurrence, $\exists K' \subset G/_H$ K' sous-groupe d'ordre p^{k-1}
Soit $\pi : G \to G/_H$ et $K = \pi^{-1}(K')$. $K \supset H$ et $\pi|_K : K \longrightarrow K'$
donc $K/_H \simeq K' \Rightarrow \# K = p^k$

$K \downarrow K/_H \nearrow K'$ ($\sim$ groupes)

CQFD

Def | Soit p un nombre premier.

- Un p-groupe (ou groupe p-primaire) est un groupe fini d'ordre p^α
- Si $H \subset G$, H est un p-groupe, on dira que c'est un p-sous-groupe de G.
- Si $H \subset G$ est un p-sous-groupe de G de cardinal p^n où p^n est la plus grande puissance de p qui divise $\# G$, alors H sera dit "un p sous-groupe de Sylow".

(NB : $H \subset G$ est un p sous-groupe de Sylow ssi c'est un p-sous-groupe maximal.)

Co | Soit G un groupe fini et $p \in \mathcal{P}$ $p | \# G$. Alors il existe un p-sous-groupe de Sylow de G.

Exercices :

① Tout conjugué d'un p sous-groupe de Sylow est encore un p sous-groupe de Sylow.

[$H \subset G$ $\# H = p^n$ où $\# G = n = p^n m$ $\Delta(p,m)=1$. $H' = gHg^{-1} = \varphi_g(H)$ où $\varphi_g(x) = gxg^{-1}$ est un automorphisme intérieur. φ_g est bijectif, donc conserve le cardinal].

② Soit G un groupe abélien fini de cardinal n.

$\exists m \in \mathbb{N}^* \, / \, \forall g \in G \quad mg = 0 \quad \Rightarrow \exists k \in \mathbb{N} \quad n \mid m^k$

[Par récurrence sur m. Soit $g \in G$, $g \neq 0$ et $H = \langle g \rangle$. $\# G/H < n$
G/H est un groupe, et $m\dot{g} = \dot{0}$ $\forall \dot{g} \in G/H$. D'après l'hypothèse de récurrence, $\# G/H \mid m^k$ or $\# G/H = \frac{\# G}{\# H} = \frac{n}{\# H}$ et $\# H \mid m$

d'où $\frac{n}{\# H} \mid m^k \Leftrightarrow m^k = \lambda \frac{n}{\# H}$ et ~~#H~~ $m = \mu \, \# H$ d'où $m^{k+1} = \mu \lambda n \Leftrightarrow n \mid m^{k+1}$]

Th 3 | Si P est un p sous-groupe de Sylow d'un groupe fini, alors tout p-sous-groupe de $N(P)$ est contenu dans P.

(Rappel : $N(H) = \{ g \in G \, / \, gHg^{-1} = H \}$)

preuve : Soit R un p sous-groupe contenu dans $N(P)$. Comme $P \triangleleft N(P)$ et $R \subset N(P)$
$R/_{P \cap R} \simeq PR/_P$. Or $\#(R/_{P\cap R}) = p^\alpha \Rightarrow \# PR/_P = p^\alpha$ et a fortiori $\#(PR) = p^\beta$
P.R est donc un p-groupe de G, et il contient P. Mais P est un p sous-groupe de Sylow, donc maximal parmi les p-sous-groupes, d'où $PR = P \Rightarrow R \subset P$

Th 4 | Soit H un sous-groupe du groupe fini G
Alors :

H = p-sous-groupe de Sylow $\Longleftrightarrow$ H = maximal dans l'ensemble des p-groupes de G ordonné par l'inclusion.

($\Rightarrow$) $\# H = p^k$ où $n = p^k m$ $\Delta(m,p) = 1$.
Soit K un p-sousgroupe de G contenant H. $\# K = p^\alpha$
$H \subset K \Rightarrow k \leq \alpha$
K sous-groupe de G $\Rightarrow \alpha \leq k$ $\Big\} \Rightarrow \# K = p^k = \# H \Rightarrow H = K$
Donc H est maximal.

($\Leftarrow$) Soit H un p-groupe maximal de G. Posons $\# H = p^\alpha$.
$\exists K$ p-sgroupe de Sylow de G : $\# K = p^k$ où $n = p^k n'$
Soit $\Lambda = \{ x \in G \, / \, x^{p^k} = e \}$. Λ est un p-sous-groupe de G, et il est clair que $H \subset \Lambda \underset{(max)}{\Rightarrow} H = \Lambda$

Or $K \subset \Lambda = H$ et $\# K = p^k \geq \# H = p^\alpha$ $\Rightarrow$ $K = H$ est un p-groupe de Sylow.

faux si G n'est pas commutatif.

2% Théorème de Cauchy

On généralise le Th 1 précédent :

Th (de Cauchy) Soit G un groupe fini d'ordre n et p un diviseur premier de n. G possède un élément d'ordre p.

preuve : récurrence sur $\# G = n$. Si $n = 2$, $G = \mathbb{Z}/2\mathbb{Z}$ et l'assertion est vraie. Supposons la démontrée pour tout $m < n$. Soit $p \mid n$, $p \in \mathcal{P}$.
Si $G = Z(G)$, le résultat est vrai (cf. Th 1)
Supposons $G \neq Z(G)$. De 2 choses l'une :

a) $\exists x \in G \setminus Z(G)$ tel que $p \mid \# H_x$

(Ici, H_x = stabilisateur de x pour la conjugaison $= \{ g \in G \,/\, g^{-1} x g = x \}$ on le nomme aussi le centralisateur de G.)
Mais $x \notin Z(G) \Rightarrow H_x \subsetneq G \Rightarrow \# H_x < \# G$ et d'après l'hypothèse de récurrence, il existe un élément d'ordre p dans H_x, donc dans G.

b) $\forall x \in G \setminus Z(G)$, $p \nmid \# H_x$

Mais $p \in \mathcal{P}$ divise $n = \# G = \# G/_{H_x} \cdot \# H_x$ et $p \nmid \# H_x$, donc $p \mid \# G/_{H_x}$ pour tout $x \notin Z(G)$
D'après l'équation des classes :

$$\# G - \sum_{x \in A} \# G/_{H_x} = \# Z(G)$$

donc $p \mid \# Z(G)$ et $Z(G)$ est commutatif ! Le Th 1 nous donne l'existence d'un élément d'ordre p dans $Z(G)$, donc dans G.
CQFD

<u>Exemple</u> : Dans S_4, il y a un élément d'ordre 2 et un d'ordre 3.
En effet : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$; $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

Ce théorème permet de donner une équivalence précieuse entre définitions :

Pro Soit G un groupe fini. Alors :

$$\# G = p^k \iff \{ \forall x \in G \ \exists \alpha \in \mathbb{N} \quad p^\alpha x = 0 \}$$

(NB : d'où une autre définition d'un p-groupe, si G est un groupe fini. Dans le cas où G est infini, G est dit p-groupe si $\forall x \in G \ \exists \alpha \,/\, \omega(x) = p^\alpha$, et la définition de "droite" s'avère plus généralisable ...)

- Si $\# G = p^k$ $\forall x \in G$ $\langle x \rangle \subset G \Rightarrow \omega(x) = p^\alpha$ (Th. Lagrange)
- Inversement, si $\forall x \in G$ $\exists \alpha$ $p^\alpha x = 0$, supposons que $q \in \mathcal{P}$ $q \mid \# G$.

D'après le théorème de Cauchy ci-dessus, G possède un élément d'ordre q. Donc $\exists \alpha \,/\, q = p^\alpha$ et $q \in \mathcal{P} \Rightarrow \alpha = 1$. Ainsi $q = p \Rightarrow \# G = p^k$.

3% <u>Dénombrement des p-groupes de Sylow</u>

Th 5 Deux p-sous-groupes de Sylow d'un groupe fini G sont conjugués dans G.
Le nombre de p-sous-groupes de Sylow de G est de la forme $1 + kp$.

(NB : on sait déjà que si H est un p-sous groupe de Sylow, alors tous les conjugués de H sont <u>aussi</u> des p-sous-groupes de Sylow)

Deux parties :

1e partie : On montre que $\# \mathcal{O} = r \equiv 1 \, [p]$

G opère sur $\mathcal{H}$ ensemble des sous-groupes de G, par conjugaison : $G \times \mathcal{H} \longrightarrow \mathcal{H}$
$g, H \longmapsto gHg^{-1}$

P = p-groupe de Sylow

$N(P) = G_P = \{g \in G \, / \, gPg^{-1} = P\}$ = groupe d'isotropie, ou stabilisateur, de P.
(NB : ici, il est égal au normalisateur de P)

On désigne par $\mathcal{O}$ l'orbite de P. On a : $\# \mathcal{O} = r = \frac{\# G}{\# N(P)}$

P opère sur $\mathcal{O}$ par conjugaison : $P \times \mathcal{O} \longrightarrow \mathcal{O}$
$h, H \longmapsto hHh^{-1}$

Soit $\mathcal{U}$ l'orbite de P sous cette action.

$$\mathcal{U} = \{O \in \mathcal{O} \, / \, \exists h \; hPh^{-1} = O\} = \{P\}$$

Ainsi $\# \mathcal{U} = 1$.

Soit $\mathcal{U}_i$ = orbite de $P_i \in \mathcal{O}$, pour $P_i \neq P$.

Si $\# \mathcal{U}_i = 1 \Rightarrow hP_ih^{-1} = P_i \quad \forall h \in P \quad \Rightarrow P \subset N(P_i)$ et d'après le théorème 3 :
$P \subset P_i$ (car P = p-sous-groupe).

Comme P est maximal dans l'ensemble des p-groupes $P \subset P_i \Rightarrow P = P_i$, ce qui est absurde.

Donc $P_i \neq P \Rightarrow \# \mathcal{U}_i \neq 1$. L'équation des classes donne :

$$\# \mathcal{O} = r = 1 + \sum_{P_i \neq P} \# \mathcal{U}_i$$

Notons H_i le stabilisateur de P_i sous l'action de P opérant sur $\mathcal{O}$ par conjugaison :

$$\# \mathcal{U}_i = \frac{\# P_i}{\# H_i} \quad \Rightarrow \# P_i = (\# \mathcal{U}_i)(\# H_i) \quad \Rightarrow \# \mathcal{U}_i \equiv 0 \, [p]$$
($\# \mathcal{U}_i \neq 1$ et P_i = p-s. groupe de Sylow)

d'où $r \equiv 1 \, [p]$. $\quad (r = \# \mathcal{O}) \quad$ (1)

2e partie : Tous les p-groupes de Sylow sont dans $\mathcal{O}$.

Soit Q un p-sous-groupe de Sylow non conjugué à P. Cela revient à dire que $Q \notin \mathcal{O}$

Q opère par conjugaison sur $\mathcal{O}$ $\quad Q \times \mathcal{O} \longrightarrow \mathcal{O}$
$(q, O) \longmapsto qOq^{-1}$

Si $\mathcal{V}_i$ = orbite de $P_i \in \mathcal{O}$, alors $\forall P_i \in \mathcal{O}$: $\# \mathcal{V}_i \neq 1$

[$\# \mathcal{V}_i = 1 \Rightarrow \forall q \in Q \quad qP_iq^{-1} = P_i \Rightarrow Q \subset N(P_i) \Rightarrow Q \subset P_i$ (th3)
donc $Q = P_i$ (cf. Q maximal)
Donc $\# \mathcal{V}_i \neq 1$]

L'équation des classes est ici : $\# \mathcal{O} = \sum \# \mathcal{V}_i$ où $\# \mathcal{V}_i = \frac{\# Q}{\# (\text{stabilisateur de } P_i)}$

$\# \mathcal{V}_i \neq 1 \Leftrightarrow \# \mathcal{V}_i > 1 \Rightarrow \# Q > \#(\text{stabilisateur de } P_i)$.

Comme $\# Q = p^n$ et que (stabilisateur de P_i) $\subset Q$ est de cardinal p^α, et comme $p^n > p^\alpha$, on en déduit que $\# \mathcal{V}_i \equiv 0 \, [p]$.

Donc $\# \mathcal{O} = \sum \# \mathcal{V}_i \equiv 0 \, [p]$ ce qui est absurde selon (1) !

Conclusion : Q = p sous-groupe de Sylow $\Rightarrow Q \in \mathcal{O}$ (orbite de P)
et $\# \mathcal{O} = r \equiv 1 \, [p]$.

Exercice : $\# G = p^k m$ où $\Delta(m, p) = 1$. Soit $\mathcal{S}$ l'ensemble des p-groupes de Sylow de G. Alors $\# \mathcal{S} \mid m$.

[Solution :

Pro | Soit G un p-groupe.
1) Alors $Z(G) \neq \{e\}$
2) G est résoluble.

preuve : 1) On considère l'équation des classes pour l'opération de conjugaison :
$G \times G \to G$
$(g, x) \mapsto gxg^{-1}$ $\qquad \# G = \# Z(G) + \sum_{x \in A} \underbrace{\frac{\# G}{\# H_x}}_{\# G_x}$

Comme $\# G = p^n$, $G_x \subset G \Rightarrow \# G_x \mid p^n$
et $\# G_x \neq p^n$ (sinon $G_x = G$ et $Z(G) = G$!) Donc $\# Z(G) \equiv 0 \; [p]$. (1)

2) <u>G est résoluble</u>.

Récurrence sur $\# G$.
- vrai pour $\# G = 2$ car $G = \mathbb{Z}/2\mathbb{Z}$ résoluble car commutatif.
- $Z(G) \subset G$ est un sgroupe de G et $\# G/Z(G) < \# G$ d'après (1)

Alors :
$$G/Z(G) = G'_0 \supset G'_1 \supset \dots \supset G'_n = \{e\} \qquad (2)$$
où $G'_{k+1} \triangleleft G'_k$ et G'_k / G'_{k+1} commutatif

Notons $\pi : G \to G/Z(G)$. On pose $G_i = \pi^{-1}(G'_i)$. On sait que π est une bijection croissante de l'ensemble des sous-groupes contenant $Z(G)$ sur l'ensemble des sous-groupes de $G/Z(G)$. Ainsi (2) $\Rightarrow$
$$G = G_0 \supset G_1 \supset \dots \supset G_n = \pi^{-1}\{e\} = Z(G)$$
et $\begin{cases} \bullet \; G_{k+1} \triangleleft G_k \\ \bullet \; G_k / G_{k+1} \simeq G'_k / G'_{k+1} \end{cases}$

CQFD

[NB : • $\forall x \in G_k \; \forall g \in G_{k+1}$, $\dot{\overline{xgx^{-1}}} \in G'_{k+1} \Rightarrow \dot{\overline{xgx^{-1}}} = \dot{g}'$ $g' \in G_{k+1}$
c.à.d $xgx^{-1}g'^{-1} \in Z(G) \subset G_{k+1} \Rightarrow xgx^{-1} \in G_{k+1}$.

• Considérons $\overline{\pi} : G_i / G_{i+1} \longrightarrow G'_i / G'_{i+1}$. C'est un isomorphisme.
$\qquad \dot{x} \longmapsto \overline{\pi(x)}$

* $\overline{\pi}$ est bien définie car $\dot{x} = \dot{y} \Leftrightarrow xy^{-1} \in G_{i+1} \Rightarrow \pi(x)\pi(y)^{-1} \in G'_{i+1} \Leftrightarrow \overline{\pi(x)} = \overline{\pi(y)}$
* $\overline{\pi}$ surjective.
* $\overline{\pi}$ injective : car $\begin{cases} \overline{\pi(x)} = \bar{0} \Leftrightarrow \pi(x) \in G'_{i+1} \Leftrightarrow x \in G_{i+1} \\ x \in G_i \end{cases} \Rightarrow \dot{x} = \dot{0}$.]

Suites normales ; Suites de Jordan-Hölder

I Préliminaire : Théorème de Zassenhaus

Th (Zassenhaus) | Si A' et B' sont respectivement 2 sous-groupes normaux de 2 sous-groupes A et B d'un groupe, alors :
* $A'(A \cap B') \triangleleft A'(A \cap B)$
* $B'(A' \cap B) \triangleleft B'(A \cap B)$
* $$A'(A\cap B) / A'(A \cap B') \simeq B'(A \cap B) / B'(A' \cap B)$$

preuve : Posons $G' = A \cap B$ et $G'' = (A' \cap B)(A \cap B')$

• Alors $G'' \triangleleft G'$: Il est clair que $G'' \subset A \cap B = G'$. D'autre part :
$A' \cap B \subset A \cap B$ et $A' \triangleleft A \Rightarrow A' \cap B \triangleleft A \cap B = G'$
$A \cap B' \subset A \cap B$ et $B' \triangleleft B \Rightarrow A \cap B' \triangleleft A \cap B = G'$

Comme $\begin{cases} U \triangleleft G' \\ V \triangleleft G' \end{cases} \Rightarrow UV \triangleleft G'$, ici : $(A' \cap B)(A \cap B') \triangleleft G' \Leftrightarrow G'' \triangleleft G'$.

• Définissons φ : $A'G' \longrightarrow G'/G''$
$a'g' \longmapsto g'G''$

L'application φ ne dépend pas de a' et g' puisque :
$a'g' = a'_1 g'_1 \Leftrightarrow a'^{-1}_1 a' = g'_1 g'^{-1} \in A' \cap G' \subset A' \cap B \subset G'' \Rightarrow g'_1 G'' = g' G''$

φ est un morphisme de groupes, surjectif : La surjectivité est évidente. D'autre part : $\exists a''_1 \in A' \,/\, g' a'_1 = a''_1 g'$ (car $A' \triangleleft G'$)

$$\varphi(a'g'a'_1g'_1) = \varphi(a'a''_1 \, g'g'_1) = g'g'_1 G'' = \varphi(a'g')\varphi(a'_1 g'_1)$$

D'autre part : $\mathrm{Ker}\,\varphi = \{a'g' \,/\, g' \in G''\} = A'G''$. Par décomposition canonique du morphisme φ :

$$\begin{array}{ccccc} A'G' & \xrightarrow{\varphi} & G'/G'' & \longrightarrow & 0 \\ \pi \downarrow & \nearrow \sim & & & \\ A'G'/A'G'' & & & & \end{array}$$

donc $A'G'/A'G'' \simeq G'/G''$

• De la même façon, on prouve que $B'G'/B'G'' \simeq G'/G''$. Par suite : $A'G'/A'G'' \simeq B'G'/B'G''$ (1)

• Or : $A'G' = A'(A \cap B)$
$B'G' = B'(A \cap B)$
et : $\begin{cases} A'G'' = A'(A' \cap B)(A \cap B') \subset A'(A \cap B') \\ A'(A \cap B') \subset A'G'' \end{cases} \Rightarrow A'G'' = A'(A \cap B')$

de la même façon $B'G'' = B'(A' \cap B)$

On conclut en écrivant (1) :

$$(1) \quad A'(A \cap B) / A'(A \cap B') \simeq B'(A \cap B) / B'(A' \cap B)$$ CQFD

(NB : On a montré, dans la décomposition canonique, que
$A'(A \cap B') = \mathrm{Ker}\,\varphi \Rightarrow A'(A \cap B') \triangleleft A'(A \cap B)$ d'où 1) et 2).)

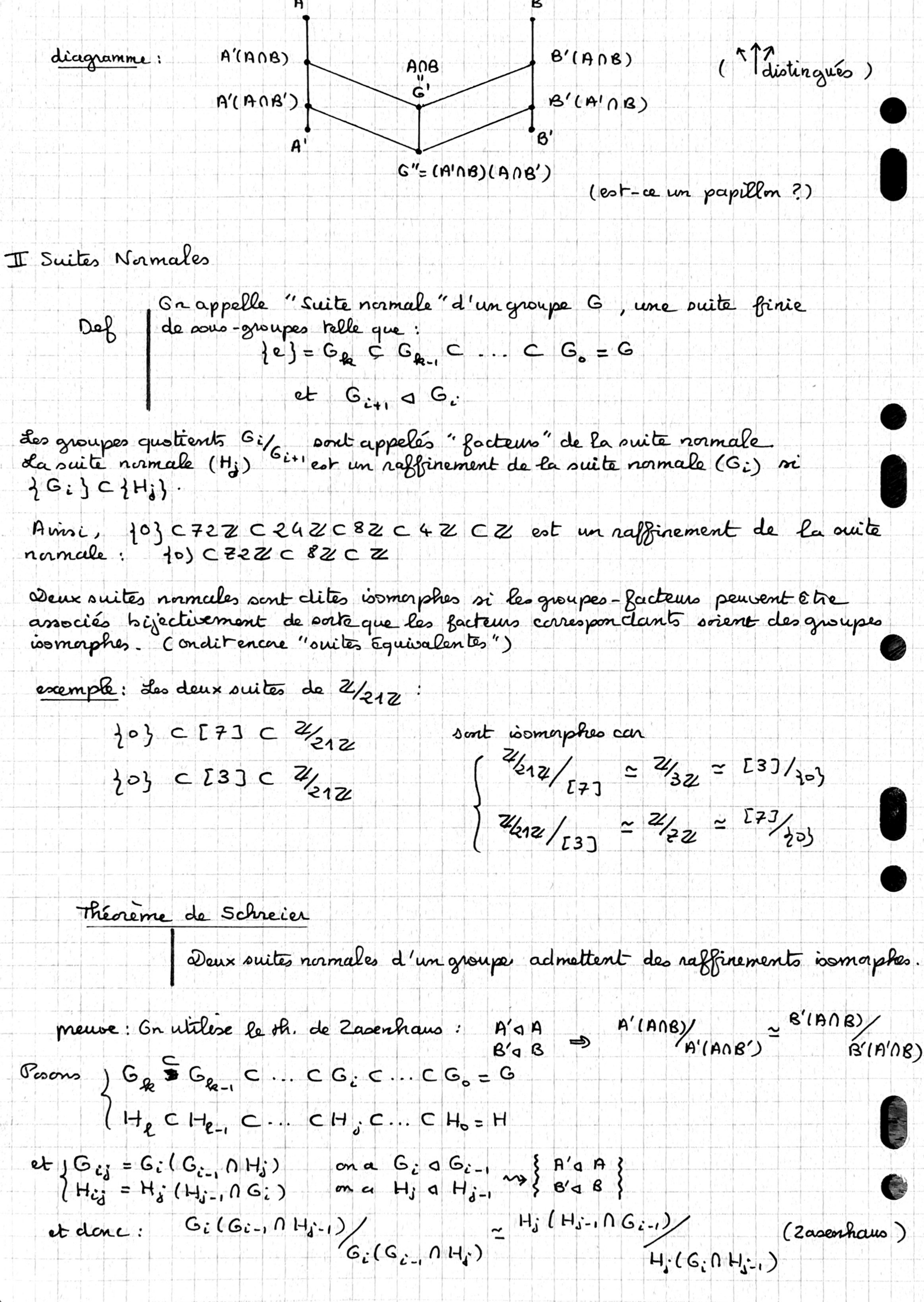


diagramme :

(↑↑↑ distingués)

(est-ce un papillon ?)

II Suites Normales

Def | On appelle "suite normale" d'un groupe G, une suite finie de sous-groupes telle que :

$$\{e\} = G_k \subsetneq G_{k-1} \subset \dots \subset G_0 = G$$

et $G_{i+1} \triangleleft G_i$

Les groupes quotients G_i/G_{i+1} sont appelés "facteurs" de la suite normale.
La suite normale (H_j) est un raffinement de la suite normale (G_i) si $\{G_i\} \subset \{H_j\}$.

Ainsi, $\{0\} \subset 72\mathbb{Z} \subset 24\mathbb{Z} \subset 8\mathbb{Z} \subset 4\mathbb{Z} \subset \mathbb{Z}$ est un raffinement de la suite normale : $\{0\} \subset 72\mathbb{Z} \subset 8\mathbb{Z} \subset \mathbb{Z}$

Deux suites normales sont dites isomorphes si les groupes-facteurs peuvent être associés bijectivement de sorte que les facteurs correspondants soient des groupes isomorphes. (on dit encore "suites équivalentes")

<u>exemple</u> : Les deux suites de $\mathbb{Z}/21\mathbb{Z}$:

$\{0\} \subset [7] \subset \mathbb{Z}/21\mathbb{Z}$

$\{0\} \subset [3] \subset \mathbb{Z}/21\mathbb{Z}$

sont isomorphes car

$$\begin{cases} \mathbb{Z}/21\mathbb{Z} \big/ [7] \simeq \mathbb{Z}/3\mathbb{Z} \simeq [3]/\{0\} \\ \mathbb{Z}/21\mathbb{Z} \big/ [3] \simeq \mathbb{Z}/7\mathbb{Z} \simeq [7]/\{0\} \end{cases}$$

<u>Théorème de Schreier</u>

| Deux suites normales d'un groupe admettent des raffinements isomorphes.

preuve : On utilise le th. de Zassenhaus : $\begin{matrix} A' \triangleleft A \\ B' \triangleleft B \end{matrix} \Rightarrow A'(A\cap B) \big/ A'(A\cap B') \simeq B'(A\cap B) \big/ B'(A'\cap B)$

Posons $\begin{cases} G_k \subsetneq G_{k-1} \subset \dots \subset G_i \subset \dots \subset G_0 = G \\ H_\ell \subset H_{\ell-1} \subset \dots \subset H_j \subset \dots \subset H_0 = H \end{cases}$

et $\begin{cases} G_{ij} = G_i(G_{i-1} \cap H_j) \\ H_{ij} = H_j(H_{j-1} \cap G_i) \end{cases}$ on a $G_i \triangleleft G_{i-1}$, on a $H_j \triangleleft H_{j-1}$ ⇝ $\begin{Bmatrix} A' \triangleleft A \\ B' \triangleleft B \end{Bmatrix}$

et donc : $G_i(G_{i-1} \cap H_{j-1}) \big/ G_i(G_{i-1} \cap H_j) \simeq H_j(H_{j-1} \cap G_{i-1}) \big/ H_j(G_i \cap H_{j-1})$ (Zassenhaus)

donc : $G_{i,j-1}/G_{ij} \simeq H_{i-1,j}/H_{ij}$ (2)

On peut formuler les suites partielles : $\begin{cases} G_{i-1} = G_{i,0} \supset G_{i,1} \supset \dots \supset G_{i,l} = G_i \\ H_{j-1} = H_{0,j} \supset H_{1,j} \supset \dots \supset H_{k,j} = H_j \end{cases}$

On introduit entre G_{i-1} et G_i les l sous-groupes G_{ij} $(1 \leq j \leq l-1)$, ceci pour i variant de 0 à k. On fait de même pour les suites (H_j). On obtient 2 suites à kl termes, qui sont isomorphes (cf. (2).)

III Suites de Jordan - Hölder.

Définition : On appelle SUITE DE JORDAN - HÖLDER, ou "suite de décomposition" du groupe G, une suite normale qui n'admet aucun raffinement ≠.

Théorème de Jordan - Hölder :

> Deux suites de Jordan - Hölder d'un groupe G sont isomorphes.

preuve :
D'après le théorème de Schreier, deux suites de décompositions admettent 2 raffinements isomorphes. Comme les seuls raffinements de ces 2 suites sont elles-mêmes, ces 2 suites sont isomorphes.

Pro | Soit $\{e\} \subset G_l \subset \dots \subset G_0 = G$ une suite normale de G
Les propositions suivantes sont ~ :
α) (G_i) est une suite de J-H
β) G_i est un sgroupe normal maximal de G_{i-1} $(\forall i)$
γ) G_{i-1}/G_i est simple $(\forall i)$

preuve : α) ⟺ β) : facile.
β) ⟺ γ) on montre, en effet, que si $H \subset G$ est un sous-groupe normal de G, et si $\pi : \mathcal{S} \longrightarrow sgr(G/H)$, $K \longmapsto \pi(K)$
est la bijection croissante de l'ensemble des sous-groupes de G contenant H sur l'ensemble des sous-groupes de G/H, alors :
$$K \triangleleft G \iff \pi(K) \triangleleft G/H \qquad \text{(laissé au lecteur)}$$
l'équivalence en découle.

(NB : On dit qu'un groupe G est "simple" s'il ne possède pas de sous-groupes distingués non triviaux)

Pro | Tout groupe fini admet une suite de Jordan - Hölder

preuve : Si $G \neq \{e\}$, il existe un sous-groupe normal maximal H_1 dans l'ensemble des sous-groupes normaux de G distincts de G. Lorsque $H_n \neq \{e\}$, on définit par récurrence H_{n+1} comme élément maximal de l'ensemble des s-groupes normaux de H_n.
$\# H_n$ décroit, donc il existe n tel que $\# H_n = 1 \iff H_n = \{e\}$, et la suite des (H_i) est, d'après sa construction, une suite de Jordan - Hölder.